UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,569	04/18/2005	Tao Zhang	11005.0065-00000	1394

97664 7590 12/06/2010

Huawei Technologies Co., Ltd./Finnegan
901 New York Avenue
NW
Washington, DC 20001

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/06/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/531,569	ZHANG ET AL.	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 September 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5 and 7-10 are pending.

Information Disclosure Statement

2. The IDS submitted on 04/18/2005 and 08/10/2006 have been considered and initialized copy attached herein.

3. The examiner verifies that all claims pending currently have no 101 problems.

Response to Amendment

4. The objection to claims 4, 8 and 10 is withdrawn in view of applicant's amendment.

Response to Arguments

Applicant's amendments and arguments are fully considered but art not persuasive.

Regarding argument Cuervo et al.'s 'session key' can not be 'authentication key' argument is not persuasive because the session key of Cuervo et al. is authentication key because: the correct key is required for proper encryption and decryption; and the session key is used for integrity checking authentication and also spoofing protection.

Regarding applicant's argument neither of the cited sections of Cuervo teach "security data package", is certainly not persuasive because multiple places of the cited portions plurality of SECURITY PACKETS sent from MGC commanding the MG, e.g., the packets includes command of 'termination event'. These commands are detailed through out the cited sections. See for ex. 7.1: the command security packet(s) comprising audit descriptors parameters that specifies auditing MG, specifying parameters values, control

descriptors, event descriptors that the MG is requested by MGC to detect and provide events, signalsdescriptors that asks the MG to apply termination, notify command, and ….; these signals are defined in the security package including timestamp and transmitted to the MG. The packets are sent in secure that the header affords data origin authentication, connection integrity, anti-replay protection of the packets passed from the MGC to the MG. For ex. the ESP header provides confidentiality of messages, using plurality of security protocols the security packages are exchanged [see sec. 7 and 10]. In view of the above the reference(s) teach 'configuring the MG with an authentication key and setting a security data package, which is a collection of a security authentication signal and an event, on a network protocol by MGC'.

Regarding argument Cuervo failure to teach 'the ICV contained in the authentication request', argument is not persuasive because the ICV of Cuervo is included in the authentication request in order to perform the integrity check or [see par. 10.2] the request message is using an AH header defined within IPSec implemented H.248 protocol and the header containing integrity check value parameter "ICV" to prevent spoofing and enhance integrity between the MG and MGC during authentication.

Regarding argument no teaching of Cuervo to check whether the MG is legal, argument is not persuasive because it is disclosed on sec. 10 that the MGC checking the integrity of the MG using the encrypted message exchanged and based on the returned response packet

obtained according to the security authentication parameter and the authentication key by the MGC [see sec. 7 and 10].

The examiner is not trying to teach the applicant's invention but rather provides a broad and reasonable interpretation for the recited claims limitations in light of the applicant's disclosure. The office does not read the disclosure or applicants arguments into the claims either.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-5 and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Network Working group, RFC 3015, Megaco protocol Version 1.0, November 2000, herein after [Cuervo et al.] in view of Matsuzaki et al. USPN 6058476.**

Regarding claims 1, 7 and 9, Cuervo et al. teaches authentication method for network security **(see sec. 10.1-10.2; The AH header defined within H.248 protocol affording data origin authentication, integrity, anti-replay message protection between MG and MGC, … ESP**

header providing confidentially of messages … AH algorithm for integrity checking between MG an MGC), comprising the following steps:

configuring a Media Gateway (MG) with an authentication key **[see sec. 10.3; the protocol. Allowing the MGC to provide and configure session key to MG]** and setting a security data package, which is a collection of security authentication signal and an event **[see sec. 7 and 10]** on a network protocol, by a Media Gateway Controller (MGC) **[see sec. 7 and 10; the MG's plurality of security packets are set by MGC]**;

during a security authentication, sending by the MGC a security authentication request **[see sec. 10.1; the MGC requesting an ESP encryption service to MG for integrity checking and for spoofing protection]** containing a security authentication parameter to the MG using the security data package **[see par. 10.2; the request message is using an AH header defined within IPSec implemented H.248 protocol and the header containing integrity check value parameter "ICV" to prevent spoofing and enhance integrity between the MG and MGC during authentication]**;

performing an encryption calculation according to the authentication key **[see 10.2-10.3; encryption authentication is requested by MGC and the MG performing encryption according to the request and configured key]** and reporting to the MGC, by the MG **[see 8.2; the MGC is expecting and receiving a response to every request]**; and

determining by the MGC whether the MG is legal based *on the returned response packet obtained according to the security authentication parameter and the authentication key* by the

MGC **[sec. 10; the MGC checks the integrity of the MG using the encrypted messages exchanged … ICV is used for integrity checking and further see sec. 7]**.

Cuervo teaches requesting encryption authentication by MGC and the MG performing encryption according to the request [see 10.2-10.3] but does not specifically explain performing encryption according to the security authentication parameter/ICV and reporting a calculation result to the MGC; and determining by the MGC whether the MG is legal by comparing the calculation result with a result calculated by the MGC.

However, Matsuzaki et al. teaches performing encryption is according to the security authentication parameter **[see col. 12 lines 28-41; first encryption IC 54 of the first device encrypting 'see fig. 3 E(S,C2)' according to received security parameter "R2R4" of C2 and received key "S" 'see fig. 3 C2=D(S,R2R4)']** and reporting a calculation result to the MGC **[see col. 12 lines 28-35 and fig. 3; First device transmitting the calculated RR2 to the Second device]**; and determining by the second device whether the first device is legal by comparing the calculation result with a result calculated by the second device **[see col. 12 lines 36-41 and fig. 3; the received RR2 is matched with the RR2 generated by MPU 55 of the Second device and legitimacy is verified if match]**.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify Cuervo et al. to authenticate legal MG utilizing the method of Matusuzaki that authenticate the legitimacy of the first device by a second device.

Regarding claim 2, Cuervo et al. teaches the authentication method for network security, wherein said network protocol is Media Gateway Control Protocol (MGCP) **[see sec. 10.2 and abstract on page 1]**.

Regarding claim 3, Cuervo et al. teaches the authentication method for network security, wherein said network protocol is H248 protocol **[see sec. 10.2 and abstract on page 1; H.248 protocol]**.

Regarding claims 4, 8 and 10 the combination teaches the authentication method for network security, wherein said data package comprises a security authentication request signal **[see Cuervo sec. 10.1; the MGC requesting an ESP encryption service to MG for integrity checking and for spoofing protection]** and a security authentication completion event **[see Matsuzaki et al. col. 13 lines 6-36; cj and also see Cuervo Appendix C]**, said security authentication request signal comprises a security authentication parameter **[fig. 3 of Matsuzaki et al. random number]**, and said security authentication completion event comprises a security authentication result parameter **[see cj on fig. 3 of Matsuzaki et al. upon receiving cj the first and second device are completing authentication and verifying trust then exchange messages];** and wherein the step of reporting a calculation result includes reporting by the MG the calculation result to the MGC via a security authentication completion event in a data package **[see cj, RR2, RR1 on fig. 3 of Matsuzaki et al. and Cuervo sec. 10].**

Regarding claim 5 Matsuzaki et al. teaches an authentication method for network security, wherein the security authentication parameter is a random number **[see fig. 3; 64 and 32 bits random numbers]**. It would have been obvious to use random number security authentication parameter to provide RANDOMIZED AUTHENTICAITON, at the time of the invention was made.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 6:00am-2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2436